



Cisco Secure ACS
インストレーション ユーザ ガイド
(パスワード変更に対応)

Release 4.0
November 2005



このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。見当たらない場合には、代理店にご連絡ください。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB (University of California, Berkeley) パブリックドメインバージョンとして、UCB が開発したプログラムを最適化したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、すべてのマニュアルおよび上記各社のソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記各社は、商品性や特定の目的への適合性、権利を侵害しないことに関する、または取り扱い、使用、または取り引きによって発生する、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその代理店は、このマニュアルの使用またはこのマニュアルを使用できないことによって起こる制約、利益の損失、データの損傷など間接的で偶発的に起こる特殊な損害のあらゆる可能性がシスコまたは代理店に知らされていても、それらに対する責任を一切負いません。

CCIP、Cisco Arrow のロゴ、Cisco Powered Network のマーク、Cisco Systems Verified のロゴ、Cisco Unity、Follow Me Browsing、FormShare、Internet Quotient、iQ Breakthrough、iQ Expertise、iQ FastTrack、iQ のロゴ、iQ Net Readiness Scorecard、Networking Academy、ScriptShare、SMARTnet、TransPath、および Voice LAN は、Cisco Systems, Inc. の商標です。Changing the Way We Work, Live, Play, and Learn、Discover All That's Possible、The Fastest Way to Increase Your Internet Quotient、および iQuick Study は、Cisco Systems, Inc. のサービスマークです。Aironet、ASIST、BPX、Catalyst、CCDA、CCDP、CCIE、CCNA、CCNP、Cisco、Cisco Certified Internetwork Expert のロゴ、Cisco IOS、Cisco IOS のロゴ、Cisco Press、Cisco Systems、Cisco Systems Capital、Cisco Systems のロゴ、Empowering the Internet Generation、Enterprise/Solver、EtherChannel、EtherSwitch、Fast Step、GigaStack、IOS、IP/TV、LightStream、MGX、MICA、Networkers のロゴ、Network Registrar、Packet、PIX、Post-Routing、Pre-Routing、RateMUX、Registrar、SlideCast、StrataView Plus、Stratm、SwitchProbe、TeleRouter、および VCO は、米国および一部の国における Cisco Systems, Inc. とその関連会社の登録商標です。

このマニュアルおよび Web サイトで言及されているその他の商標はすべて、それぞれの所有者のもです。「パートナー」という語の使用は、シスコと他社の提携関係を意味するものではありません。(0206R)

Cisco Secure ACS インストール ユーザガイド (パスワード変更に対応)

Copyright © 2003–2005, Cisco Systems, Inc.

All rights reserved.



このマニュアルについて	v
対象読者	v
表記法	vi
製品マニュアル	vii
関連資料	viii
技術情報の入手方法	viii
Cisco.com	viii
Product Documentation DVD (英語版)	viii
マニュアルの発注方法 (英語版)	ix
シスコシステムズマニュアルセンター	ix
シスコ製品のセキュリティの概要	x
シスコ製品のセキュリティ問題の報告	x
テクニカル サポート	xi
Cisco Technical Support & Documentation Web サイト	xi
Japan TAC Web サイト	xi
サービス リクエストの発行	xii
サービス リクエストのシビラティの定義	xii
その他の資料および情報の入手方法	xiii

CHAPTER 1

Cisco Secure ACS の User-Changeable Password のインストールと使用	1-1
UCP について	1-2
SSL について	1-2
UCP のインストール	1-3
Web サーバの準備	1-3
UCP 向けの Cisco Secure ACS の準備	1-4
Web サーバでの SSL のイネーブル化	1-6
UCP ソフトウェアのインストール	1-6
UCP URL の特定	1-8
UCP のアップグレード	1-9
UCP のアンインストール	1-9
パスワードの変更	1-10



このマニュアルについて

このガイドでは、Cisco Secure Access Control Server Release 4.0 for Windows(ACS)の User-Changeable Password をインストール、設定、および使用する方法を説明します。

対象読者

このガイドは、User-Changeable Password をインストールおよび設定し、ACS Release 4.0 で使用するネットワーク管理者を対象としています。また、User-Changeable Password の Web サイトにアクセスし、ACS パスワードを変更するネットワーク ユーザのための情報も記載されています。

表記法

このマニュアルは、次の表記法を使用しています。

項目	表記法
手順の実行中に選択する必要があるコマンド、キーワード、専門用語、およびオプション	太字
ユーザが値を指定する変数、および新しい用語や重要な用語	イタリック体
セッション情報、システム情報、パス、およびファイル名の表示出力	<code>screen</code> フォント
ユーザが入力する情報	太字の <code>screen</code> フォント
ユーザが入力する変数	イタリック体の <code>screen</code> フォント
メニュー項目およびボタン名	太字
メニュー項目の選択順序	Option > Network Preferences



ヒント

ご使用の製品を有効活用するために役立つヒントを示しています。



(注)

「注釈」です。作業を続行する前に確認すべき重要な情報や役立つ情報、このマニュアル以外の参照資料などを紹介しています。



注意

「要注意」の意味です。機器の損傷、データの損失、またはネットワークセキュリティの侵害を予防するための注意事項が記述されています。



警告

怪我、ソフトウェアの破壊、または機器の損傷を防止するために留意すべき情報を示しています。この記号がある場合、記載されている情報に従って慎重に作業しないと、明らかなセキュリティ侵害につながります。

製品マニュアル



(注) 初版発行後、印刷物または電子マニュアルのアップデートを行う場合があります。マニュアルのアップデートについては、Cisco.com で確認してください。

表 1 に、ご利用可能な製品マニュアルを示します。

表 1 製品マニュアル

マニュアル タイトル	ご利用形式
<i>Release Notes for Cisco Secure ACS Solution Engine</i>	<ul style="list-style-type: none"> 製品に同梱されている印刷マニュアル Cisco.com
<i>Release Notes for Cisco Secure ACS for Windows Server</i>	<ul style="list-style-type: none"> 製品に同梱されている印刷マニュアル Cisco.com
<i>Installation and Setup Guide for Cisco Secure ACS Solution Engine</i>	<ul style="list-style-type: none"> 製品 CD-ROM に収録されている PDF Cisco.com 印刷マニュアルの注文 (Part Number DOC-7816532)¹
<i>Installation Guide for Cisco Secure ACS for Windows Server</i>	<ul style="list-style-type: none"> 製品 CD-ROM に収録されている PDF Cisco.com 印刷マニュアルの注文 (Part Number DOC-7816529)¹
<i>User Guide for Cisco Secure ACS Solution Engine</i>	<ul style="list-style-type: none"> 製品 CD-ROM に収録されている PDF Cisco.com 印刷マニュアルの注文 (Part Number DOC-7816534)¹
<i>User Guide for Cisco Secure ACS for Windows Server</i>	<ul style="list-style-type: none"> 製品 CD-ROM に収録されている PDF Cisco.com 印刷マニュアルの注文 (Part Number DOC-7816592)¹
<i>Installation and User Guide for Cisco Secure ACS User-Changeable Passwords</i>	<ul style="list-style-type: none"> 製品 CD-ROM に収録されている PDF Cisco.com
<i>Regulatory Compliance and Safety Information for Cisco Secure ACS Solution Engine</i>	<ul style="list-style-type: none"> 製品に同梱されている印刷マニュアル 製品 CD-ROM に収録されている PDF Cisco.com
<i>Supported and Interoperable Devices and Software Tables for Cisco Secure ACS Solution Engine</i>	Cisco.com
<i>Recommended Resources for the Cisco Secure ACS User</i>	Cisco.com
オンライン マニュアル	Cisco Secure ACS の HTML インターフェイスで Online Documentation をクリック

1. P.viii の「技術情報の入手方法」を参照してください。

関連資料



(注)

初版発行後、印刷物または電子マニュアルのアップデートを行う場合があります。マニュアルのアップデートについては、Cisco.com で確認してください。

Cisco Secure ACS for Windows Server に関する White Paper を参照するには、次の URL にアクセスしてください。

http://www.cisco.com/en/US/partner/products/sw/secursw/ps2086/prod_white_papers_list.html

技術情報の入手方法

シスコの製品マニュアルやその他の資料は、Cisco.com でご利用いただけます。また、テクニカルサポートおよびその他のリソースを、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法について説明します。

Cisco.com

次の URL から、シスコ製品の最新資料を入手することができます。

<http://www.cisco.com/techsupport>

シスコの Web サイトには、次の URL からアクセスしてください。

<http://www.cisco.com>

また、シスコの Web サイトの各国語版へは、次の URL からアクセスできます。

http://www.cisco.com/public/countries_languages.shtml

シスコ製品の最新資料の日本語版は、次の URL からアクセスしてください。

<http://www.cisco.com/jp>

Product Documentation DVD (英語版)

シスコ製品のマニュアルおよびその他の資料は、製品に付属の Product Documentation DVD パッケージでご利用いただけます。Product Documentation DVD は定期的に更新されるので、印刷資料よりも新しい情報が得られます。

Product Documentation DVD は、技術情報を包含する製品マニュアルをポータブルなメディアに格納した、包括的なライブラリです。この DVD を使用することにより、シスコ製の各ハードウェアやソフトウェアのインストール、コンフィギュレーション、およびコマンドに関する複数のバージョンのマニュアルにアクセスし、技術情報を HTML で参照できます。また、この DVD を使用すると、シスコの Web サイトで参照できるのと同じマニュアルに、インターネットに接続せずにアクセスできます。一部の製品については、PDF 版のマニュアルもご利用いただけます。

Product Documentation DVD は、1 回単位で入手することも、または定期購読することもできます。Cisco.com 登録ユーザ (Cisco Direct Customers) の場合、次の URL の Cisco Marketplace から Product Documentation DVD (Product Number DOC-DOCDVD=) を発注できます。

<http://www.cisco.com/go/marketplace/>

マニュアルの発注方法（英語版）

2005 年 6 月 30 日以降、Cisco.com 登録ユーザの場合、Cisco Marketplace の Product Documentation Store からシスコ製品の英文マニュアルを発注できるようになっています。次の URL にアクセスしてください。

<http://www.cisco.com/go/marketplace/>

Cisco.com に登録されていない場合、製品を購入された代理店へお問い合わせください。

シスコシステムズマニュアルセンター

シスコシステムズマニュアルセンターでは、シスコ製品の日本語マニュアルの最新版を PDF 形式で公開しています。また、日本語マニュアル、および日本語マニュアル CD-ROM もオンラインで発注可能です。ご希望の方は、次の URL にアクセスしてください。

<http://www2.hipri.com/cisco/>

また、シスコシステムズマニュアルセンターでは、日本語マニュアル中の誤記、誤植に関するコメントをお受けしています。次の URL の「製品マニュアル内容不良報告」をクリックすると、コメント入力画面が表示されます。

<http://www2.hipri.com/cisco/>

なお、技術内容に関するお問い合わせは、この Web サイトではお受けできませんので、製品を購入された各代理店へお問い合わせください。

シスコ製品のセキュリティの概要

シスコでは、オンラインの Security Vulnerability Policy ポータル (英文のみ) を無料で提供しています。URL は次のとおりです。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このサイトは、次の目的に利用できます。

- シスコ製品のセキュリティ脆弱性を報告する。
- シスコ製品に伴うセキュリティ事象についてサポートを受ける。
- シスコからセキュリティ情報を受け取るための登録をする。

シスコ製品に関するセキュリティ勧告および注意事項の最新のリストには、次の URL からアクセスできます。

<http://www.cisco.com/go/psirt>

勧告および注意事項がアップデートされた時点でリアルタイムに確認する場合は、次の URL から Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) フィードにアクセスしてください。

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

シスコ製品のセキュリティ問題の報告

シスコでは、セキュアな製品を提供すべく全力を尽くしています。製品のリリース前には内部でテストを行い、すべての脆弱性を早急に修正するよう努力しています。万一、シスコ製品に脆弱性が見つかった場合は、PSIRT にご連絡ください。

- 緊急の場合 : security-alert@cisco.com (英語のみ)
緊急とは、システムがアクティブな攻撃を受けている場合、または至急の対応を要する重大なセキュリティ上の脆弱性が報告されている場合を指します。これに該当しない場合はすべて、緊急でないと見なされます。
- 緊急でない場合 : psirt@cisco.com (英語のみ)

緊急の場合は、電話で PSIRT に連絡することもできます。

- 1 877 228-7302 (英語のみ)
- 1 408 525-6532 (英語のみ)



ヒント

シスコに機密情報をお送りいただく際には、PGP (Pretty Good Privacy) または互換製品を使用して、暗号化することをお勧めします。PSIRT は、PGP バージョン 2.x から 8.x と互換性のある暗号化情報に対応しています。

無効になった、または有効期限が切れた暗号鍵は、絶対に使用しないでください。PSIRT に連絡する際に使用する正しい公開鍵には、Security Vulnerability Policy ページの Contact Summary セクションからリンクできます。次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このページ上のリンクからは、現在使用されている最新の PGP 鍵の ID にアクセスできます。

テクニカル サポート

Cisco Technical Support では、24 時間テクニカル サポートを提供しています。Cisco.com の Cisco Technical Support & Documentation Web サイトでは、多数のサポート リソースをオンラインで提供しています。また、シスコと正式なサービス契約を交わしているお客様には、Cisco Technical Assistance Center (TAC) のエンジニアが電話でのサポートにも対応します。シスコと正式なサービス契約を交わしていない場合は、代理店にお問い合わせください。

Cisco Technical Support & Documentation Web サイト

Cisco Technical Support & Documentation Web サイトでは、シスコ製品やシスコの技術に関するトラブルシューティングにお役立ていただけるように、オンラインでマニュアルやツールを提供しています。この Web サイトは、24 時間、いつでも利用可能です。URL は次のとおりです。

<http://www.cisco.com/techsupport>

Cisco Technical Support & Documentation Web サイトのツールにアクセスするには、Cisco.com のユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

<http://tools.cisco.com/RPF/register/register.do>



(注)

Web または電話でサービス リクエストを発行する前に、Cisco Product Identification (CPI) ツールを使用して製品のシリアル番号を確認してください。CPI ツールには、Cisco Technical Support & Documentation Web サイトから、Documentation & Tools の下の **Tools & Resources** リンクをクリックするとアクセスできます。アルファベット順の索引ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下の **Cisco Product Identification Tool** リンクをクリックします。CPI ツールには、3 つの検索オプションがあります。製品 ID またはモデル名による検索、ツリー表示による検索、show コマンド出力のコピー アンド ペーストによる特定製品の検索です。検索結果では、製品が図示され、シリアル番号ラベルの位置が強調表示されます。ご使用の製品でシリアル番号ラベルを確認し、その情報を記録してからサービス コールをかけてください。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト (<http://www.cisco.com/tac>) のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

<http://www.cisco.com/jp/go/tac>

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

<http://www.cisco.com/jp/register>

サービス リクエストの発行

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます (S3: ネットワークに軽微な障害が発生した、S4: 製品情報が必要である)。状況を入力すると、その状況を解決するための推奨手段が検索されます。これらの推奨手段で問題を解決できない場合は、シスコのエンジニアが対応します。TAC Service Request Tool には、次の URL からアクセスできます。

<http://www.cisco.com/techsupport/servicerequest>

S1 または S2 のサービス リクエストの場合、またはインターネットにアクセスできない場合は、Cisco TAC に電話でお問い合わせください (S1: ネットワークがダウンした、S2: ネットワークの機能が著しく低下した)。S1 および S2 のサービス リクエストには、シスコのエンジニアがすぐに割り当てられ、業務を円滑に継続できるようサポートします。

Cisco TAC の連絡先については、次の URL を参照してください。

<http://www.cisco.com/techsupport/contacts>

サービス リクエストのシビラティの定義

シスコでは、報告されるサービス リクエストを標準化するために、シビラティを定義しています。

シビラティ 1 (S1): ネットワークが「ダウン」した状態か、業務に致命的な損害が発生した場合。お客様およびシスコが、24 時間体制でこの問題を解決する必要があると判断した場合。

シビラティ 2 (S2): 既存のネットワーク動作が著しく低下したか、シスコ製品が十分に機能しないため、業務に重大な影響を及ぼした場合。お客様およびシスコが、通常の業務中の全時間を費やして、この問題を解決する必要があると判断した場合。

シビラティ 3 (S3): ネットワークの動作パフォーマンスが低下しているが、ほとんどの業務運用は継続できる場合。お客様およびシスコが、業務時間中にサービスを十分なレベルにまで復旧させる必要があると判断した場合。

シビラティ 4 (S4): シスコ製品の機能、インストレーション、コンフィギュレーションについて、情報または支援が必要な場合。業務の運用には、ほとんど影響がありません。

その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手できます。

- Cisco Marketplace では、シスコの書籍やリファレンス ガイド、マニュアル、ロゴ製品を数多く提供しています。購入を希望される場合は、次の URL にアクセスしてください。

<http://www.cisco.com/go/marketplace/>

- Cisco Press では、ネットワーク全般、トレーニング、および認定資格に関する出版物を幅広く発行しています。これらの出版物は、初級者にも上級者にも役立ちます。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。

<http://www.ciscopress.com>

- 『*Packet*』はシスコシステムズが発行する技術者向けの雑誌で、インターネットやネットワークへの投資を最大限に活用するために役立ちます。本誌は季刊誌として発行され、業界の最先端トレンド、最新テクノロジー、シスコ製品やソリューション情報が記載されています。また、ネットワーク構成およびトラブルシューティングに関するヒント、コンフィギュレーション例、カスタマー ケース スタディ、認定情報とトレーニング情報、および充実したオンラインサービスへのリンクの内容が含まれます。『*Packet*』には、次の URL からアクセスしてください。

<http://www.cisco.com/packet>

日本語版『*Packet*』は、米国版『*Packet*』と日本版のオリジナル記事で構成されています。日本語版『*Packet*』には、次の URL からアクセスしてください。

<http://www.cisco.com/japanese/warp/public/3/jp/news/packet/>

- 『*iQ Magazine*』はシスコシステムズの季刊誌で、成長企業が収益を上げ、業務を効率化し、サービスを拡大するためには技術をどのように利用したらよいかを学べるように構成されています。本誌では、実例とビジネス戦略を挙げて、成長企業が直面する問題とそれを解決するための技術を紹介し、読者が技術への投資に関して適切な決定を下せるよう配慮しています。『*iQ Magazine*』には、次の URL からアクセスしてください。

<http://www.cisco.com/go/iqmagazine>

デジタル版には、次の URL からアクセスできます。

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスしてください。

<http://www.cisco.com/ipj>

- シスコシステムズが提供するネットワーキング製品、および各種のカスタマー サポート サービスは、次の URL から入手できます。

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection は対話形式の Web サイトです。このサイトでは、ネットワーキング製品やテクノロジーに関する質問、提案、および情報をネットワーキング担当者がシスコの専門家や他のネットワーキング担当者と共に共有できます。次の URL にアクセスしてディスカッションに参加してください。

<http://www.cisco.com/discuss/networking>

- シスコは、国際的なレベルのネットワーク関連トレーニングを実施しています。最新情報については、次の URL からアクセスしてください。

<http://www.cisco.com/en/US/learning/index.html>



Cisco Secure ACS の User-Changeable Password の インストールと使用

このガイドでは、Cisco Secure Access Control Server Release 4.0 (ACS) に User-Changeable Password (UCP) をインストールして使用する方法を説明します。UCP は、次のソフトウェアで使用できます。

- Cisco Secure ACS for Windows, Release 4.0
- Cisco Secure ACS Solution Engine, Release 4.0

この章には、次の項があります。

- [UCP について \(P.1-2\)](#)
 - [SSL について \(P.1-2\)](#)
- [UCP のインストール \(P.1-3\)](#)
 - [Web サーバの準備 \(P.1-3\)](#)
 - [UCP 向けの Cisco Secure ACS の準備 \(P.1-4\)](#)
 - [Web サーバでの SSL のイネーブル化 \(P.1-6\)](#)
 - [UCP ソフトウェアのインストール \(P.1-6\)](#)
 - [UCP URL の特定 \(P.1-8\)](#)
- [UCP のアップグレード \(P.1-9\)](#)
- [UCP のアンインストール \(P.1-9\)](#)
- [パスワードの変更 \(P.1-10\)](#)

UCP について

UCP アプリケーションを使用すると、ユーザが Web ベースのユーティリティを使用して自分の ACS パスワードを変更できるようになります。パスワードを変更する必要があるときは、サポート対象の Web ブラウザを使用して UCP Web ページにアクセスできます。ACS で動作確認済みの Web ブラウザについては、ACS 製品のリリース ノートを参照してください。

UCP Web ページでは、ユーザがログインする必要があります。ここで必要なパスワードは、ユーザアカウントの Password Authentication Protocol (PAP; パスワード認証プロトコル) パスワードです。UCP が ACS のユーザ認証を行うと、ユーザは新しいパスワードを指定できるようになります。UCP はユーザの PAP パスワードと Challenge Handshake Authentication Protocol (CHAP; チャレンジ ハンドシェイク認証プロトコル) パスワードを新しいパスワードに変更します。

UCP をインストールするには、Microsoft IIS 5.0 (Windows 2000 に付属) または 6.0 (Windows Server 2003 に付属) を実行する Web サーバが必要です。

SSL について

UCP と ACS 間の通信は、128 ビット暗号化で保護されています。セキュリティを強化するために、Secure Sockets Layer (SSL) を実装して Web ブラウザと UCP の間の通信を保護することをお勧めします。SSL プロトコルを使用すると、UCP Web サーバとユーザの Web ブラウザとの間で行われるリモートアクセスのデータ転送が、セキュリティで保護されます。

ユーザは Web ブラウザと Microsoft IIS 間の接続を通じてユーザの ACS 内部データベース パスワードを変更するため、ユーザとパスワード データは攻撃を受けやすくなります。SSL プロトコルは、Web ブラウザと Microsoft IIS の間で行われるパスワードなどのデータ転送を暗号化します。

SSL は Microsoft IIS に対して、有効な認証証明書の提示を要求します。このためユーザは、認証局から証明書を取得する必要があります。公開認証局を利用する場合は、特定の要件を満たせば、有料でキーが割り当てられます。

UCP のインストール

ここでは、UCP をインストールするための情報や手順について説明します。

この項には、次のトピックがあります。

- [Web サーバの準備 \(P.1-3\)](#)
- [UCP 向けの Cisco Secure ACS の準備 \(P.1-4\)](#)
- [Web サーバでの SSL のイネーブル化 \(P.1-6\)](#)
- [UCP ソフトウェアのインストール \(P.1-6\)](#)
- [UCP URL の特定 \(P.1-8\)](#)

Web サーバの準備

Web サーバを準備するには、Web サーバ上に仮想ディレクトリを作成する必要があります。この仮想ディレクトリは、UCP セットアップ プログラムが HTML ファイルと CGI 実行ファイルを配置するファイル システム ディレクトリに対応します。

UCP 向けに準備するには、次の手順を実行します。

ステップ 1 Web サーバが Microsoft IIS 5.0 または 6.0 を使用することを確認します。

- IIS 5.0 は Windows 2000 に含まれています。
- IIS 6.0 は Windows Server 2003 に含まれています。

ステップ 2 Web サーバのホーム ディレクトリで、2 つのディレクトリを作成します。



ヒント ホーム ディレクトリを確認するには、Microsoft IIS の Default Web Site のプロパティを参照してください。

- **secure** : このディレクトリには、UCP によって使用された HTML ファイルが置かれます。secure 以外の名前を指定することもできます。ディレクトリ名は、他のインストール手順で使用できるように記録しておく必要があります。
- **securecgi-bin** : このディレクトリには、UCP によって使用された CGI 実行ファイルが置かれます。securecgi-bin 以外の名前を指定することもできます。ディレクトリ名は、他のインストール手順で使用できるように記録しておく必要があります。

たとえば、Web サーバのホーム ディレクトリが `C:\inetpub\wwwroot` の場合は、これらのディレクトリを `C:\inetpub\wwwroot` に追加します。

ステップ 3 Microsoft IIS で、UCP で使用される HTML ファイルの仮想ディレクトリを追加します。仮想ディレクトリを作成する場合は、次のように指定します。

- **仮想ディレクトリ エイリアス** : 仮想ディレクトリの名前。この仮想ディレクトリは、[ステップ 2](#) で作成した `secure` ディレクトリに対応します。ディレクトリ名を `secure` にすることをお勧めします。このエイリアスは、UCP へのアクセスに使用する URL の一部となるため、簡潔で分かりやすいエイリアスにしておくと、ユーザが URL を覚えやすくなります。
- **Web サイトのコンテンツ ディレクトリ** : 指定するディレクトリは、[ステップ 2](#) で作成した `secure` ディレクトリと一致させる必要があります。[ステップ 2](#) のデフォルト ディレクトリは、`C:\inetpub\wwwroot\secure` です。

■ UCP のインストール

- **アクセス権**：この仮想ディレクトリに読み取りアクセス権を付与します。それ以外のアクセス権は不要です。

仮想ディレクトリの作成方法については、使用しているバージョンの IIS に関するマイクロソフトのマニュアルを参照してください。

ステップ 4 UCP で使用される CGI 実行ファイルの仮想ディレクトリを追加します。仮想ディレクトリを作成する場合は、次のように指定します。

- **仮想ディレクトリエイリアス**：仮想ディレクトリの名前。この仮想ディレクトリは、[ステップ 2](#) で作成した `securecgi-bin` ディレクトリに対応します。ディレクトリ名を `securecgi-bin` にすることをお勧めします。
- **Web サイトのコンテンツ ディレクトリ**：指定するディレクトリは、[ステップ 2](#) で作成した `securecgi-bin` ディレクトリと一致させる必要があります。[ステップ 2](#) のデフォルトディレクトリは、`C:\Inetpub\wwwroot\securecgi-bin` です。
- **アクセス権**：この仮想ディレクトリに読み取りアクセス権と実行アクセス権を付与します。それ以外のアクセス権は不要です。

仮想ディレクトリの作成方法については、使用しているバージョンの IIS に関するマイクロソフトのマニュアルを参照してください。

ステップ 5 Web サーバが IIS 6.0 を実行している場合、未知の CGI 拡張機能が許可されるように IIS の設定を変更する必要があります。これを行うには、IIS Manager ウィンドウの Web Service Extension ページを使用して、**Allow Unknown CGI Extensions** のステータスを **Allowed** に設定します。

ステップ 6 Microsoft IIS 5.0 Web サーバを保護するために IIS Lockdown Tool を使用している場合は、Lockdown Tool で実行ファイルの起動が許可されていることを確認します。実行ファイルを起動できない場合、UCP が失敗し、ユーザはパスワードを変更できません。

UCP 向けの Cisco Secure ACS の準備

UCP 向けに ACS を準備するには、Web サーバが認証、認可、アカウントिंग (AAA) サーバの一種として認識されるように、ACS を設定する必要があります。この設定を実行すると、ACS は、Web サーバ上の UCP によって処理されたユーザパスワード変更を認識して、応答できるようになります。この設定を行わなかった場合、ACS は、UCP からのユーザパスワード変更の要求を無視します。



(注) ACS および Microsoft IIS ソフトウェアを同じコンピュータ上で実行する場合は、この手順を実行する必要はありません。[P.1-6 の「Web サーバでの SSL のイネーブル化」](#)に進んでください。

UCP 向けに準備するには、次の手順を実行します。

ステップ 1 UCP からのユーザパスワード変更の送信先となる、ACS の Web インターフェイスにログインします。



(注) ACS Internal Database Replication 機能を使用している場合、UCP がユーザパスワード変更を送信する先の ACS は、プライマリ ACS である必要があります。そうでない場合、ユーザデータベースを複製したときに、プライマリ ACS の古い情報がユーザパスワードの変更を上書きします。

ステップ 2 Interface Configuration > Advanced Options を選択します。

Advanced Options ページが表示されます。

ステップ 3 Distributed Systems Settings チェックボックスがオンになっていることを確認します。オンになっている場合は、Network Configurations セクションに AAA Servers テーブルが表示されます。

ステップ 4 Submit をクリックします。

ステップ 5 Network Configuration をクリックします。

ステップ 6 Network Device Group (NDG; ネットワーク デバイス グループ) がイネーブルの場合は、UCP Web サーバの追加先となる NDG をクリックします。

ステップ 7 AAA Servers テーブルの Add Entry をクリックします。

ステップ 8 AAA Server Name ボックスに、UCP Web サーバの名前を入力します。Web サーバのホスト名を使用することをお勧めします。ただし、UCP Web サーバをより簡単に識別できるように、UCP などの追加情報を入れることもできます。たとえば、Web サーバのホスト名が `wwwin` の場合、AAA Server Name ボックスに `UCP-wwwin` と入力できます。

ステップ 9 AAA Server IP Address ボックスに、UCP Web サーバの IP アドレスを入力します。ドット付き 10 進形式を使用します。



(注) Add AAA Server ページにあるその他の設定は、UCP とは関係ありません。

ステップ 10 Submit + Restart をクリックします。

ACS は、UCP のインストール先となる Web サーバからのパスワード変更情報を認識して、応答するよう設定されます。

Web サーバでの SSL のイネーブル化

ここでは、SSL をイネーブルして、ユーザの Web ブラウザと UCP を実行する Microsoft IIS の間の通信を暗号化する方法を説明します。



(注)

SSL はイネーブルにしておくことをお勧めします。すべてのユーザが例外なくセキュア境界の内側から UCP にアクセスする場合は、SSL は不要です。しかしそれ以外の場合は、ユーザの Web ブラウザと UCP を実行する Web サーバとの間の UCP トラフィックを暗号化するように、SSL をイネーブルにする必要があります。

Web サーバでオプションの SSL セキュリティをイネーブルにするには、次の手順を実行します。

ステップ 1 認証局から証明書を取得します。

ステップ 2 認証局から証明書を受け取ったら、証明書を Web サーバにインストールします。証明書のインストール方法については、使用しているバージョンの IIS に関するマイクロソフトのマニュアルを参照してください。

ステップ 3 Microsoft IIS のマニュアルに従って、Web サーバ上で SSL セキュリティを有効にします。

SSL セキュリティを有効にする場合、次の点に留意してください。

- SSL セキュリティは、Web サイトのルートに対して、または 1 つ以上の仮想ディレクトリに対してイネーブルにできます。
- SSL をイネーブルにし、正しく設定すると、SSL 対応のクライアントだけが SSL 対応の WWW ディレクトリと通信できるようになります。
- SSL 対応の WWW フォルダにあるドキュメントを指す URL では、`http://` の代わりに `https://` を使用する必要があります。URL で `http://` を使用するリンクは、セキュア ディレクトリでは動作しません。

UCP ソフトウェアのインストール

始める前に

UCP ソフトウェアのインストール プロセスには、次の要件があります。

- 次の項の手順を完了していることを確認します。
 - [Web サーバの準備 \(P.1-3\)](#)
 - [UCP 向けの Cisco Secure ACS の準備 \(P.1-4\)](#)
- SSL を実装する場合は、P.1-6 の「Web サーバでの SSL のイネーブル化」の手順を完了していることを確認します。
- ACS の CD が手元にあることを確認します。

User-Changeable Password ソフトウェアをインストールするには、次の手順を実行します。

ステップ 1 UCP をインストールする Web サーバで、ローカル管理者としてログインします。

ステップ 2 Web サーバのドライブに ACS の CD を挿入します。



ヒント autorun によって ACS のセットアップ ウィンドウが開いた場合は、Cancel をクリックします。

ステップ 3 Windows Explorer を使用して、ACS の CD にある UCP サブディレクトリを開きます。

ステップ 4 UCP の SETUP.EXE ファイルをダブルクリックします。

Before You Begin ダイアログボックスが表示されます。

ステップ 5 すべての項目のチェックボックスをオンにして、次に Next をクリックします。

Choose Destination Location ダイアログボックスに、UCP で使用される HTML ファイルのデフォルトディレクトリが表示されます。

ステップ 6 P.1-3 の「Web サーバの準備」で作成した secure ディレクトリのフルパスを指定します。ディレクトリ名として secure を選択していて、C:\Inetpub\wwwroot が Web サーバのホーム ディレクトリであるときは、デフォルトの場所をそのまま使用できます。

ステップ 7 Next をクリックします。

2 つ目の Choose Destination Location ダイアログボックスに、UCP で使用される CGI 実行ファイルのデフォルトディレクトリが表示されます。

ステップ 8 P.1-3 の「Web サーバの準備」で作成した securecgi-bin ディレクトリのフルパスを指定します。ディレクトリ名として securecgi-bin を選択していて、C:\Inetpub\wwwroot が Web サーバのホーム ディレクトリであるときは、デフォルトの場所をそのまま使用できます。

ステップ 9 Next をクリックします。

Enter Information ダイアログボックスに、Web サーバの IP アドレスを使用した、HTML 仮想ディレクトリのデフォルト URL が表示されます。

ステップ 10 HTML 仮想ディレクトリの URL を指定します。次の手順に従います。

- SSL を使用しない場合で、UCP HTML ディレクトリの仮想ディレクトリエイリアスとして secure を使用するように選択している場合は、デフォルト値をそのまま使用できます。
- SSL を使用する場合は、URL の先頭部分を `http://` から `https://` に変更します。`http` の後ろに `s` が必要です。この文字がないと、ユーザと UCP 間の通信が SSL で暗号化されません。
- UCP HTML ディレクトリの仮想ディレクトリエイリアスとして secure 以外の名前を選択している場合は、secure を、P.1-3 の「Web サーバの準備」で選択した名前に変更します。

たとえば、SSL を使用していて、HTML 仮想ディレクトリエイリアスとして ucp を指定しているときは、URL を `https://IPAddress/ucp` に変更する必要があります。IPAddress は、Web サーバのドット付き 10 進 IP アドレスです。

ステップ 11 Next をクリックします。

2 つ目の Enter Information ダイアログボックスに、Web サーバの IP アドレスを使用した、CGI 仮想ディレクトリのデフォルト URL が表示されます。

ステップ 12 次のガイドラインに従って、CGI 仮想ディレクトリの URL を指定します。

- SSL を使用しない場合で、UCP CGI ディレクトリの仮想ディレクトリ エイリアスとして `securecgi-bin` を使用するように選択している場合は、デフォルト値をそのまま使用できます。
- SSL を使用する場合は、URL の先頭部分を `http://` から `https://` に変更します。`http` の後ろに `s` が必要です。この文字がないと、ユーザと UCP 間の通信が SSL で暗号化されません。
- UCP HTML ディレクトリの仮想ディレクトリ エイリアスとして `securecgi-bin` 以外の名前を選択している場合は、`secure` を、P.1-3 の「Web サーバの準備」で選択した名前に変更します。

たとえば、SSL を使用していて、HTML 仮想ディレクトリ エイリアスとして `ucpcgi-bin` を指定しているときは、URL を `https://IPAddress/ucpcgi-bin` に変更する必要があります。IPAddress は、Web サーバのドット付き 10 進 IP アドレスです。

ステップ 13 Next をクリックします。

Connecting to Cisco Secure Server ダイアログボックスが表示されます。

ステップ 14 UCP からのユーザパスワード変更の送信先となる、ACS の IP アドレスを入力します。IP アドレスには、ドット付き 10 進形式を使用します。

ステップ 15 Next をクリックします。

指定した ACS への接続がテストされ、Setup Complete ダイアログボックスが表示されます。

ステップ 16 Finish をクリックして、インストールを完了します。

UCP がインストールされました。Web サーバが実行中かつアクセス可能な場合、ユーザは UCP を使用して ACS のパスワードを変更できます。UCP へのアクセスについては、P.1-8 の「UCP URL の特定」を参照してください。

UCP URL の特定

UCP のインストールが正常に終了したら、サポート対象の Web ブラウザを使用して UCP にアクセスできます。サポート対象の Web ブラウザのリストについては、アクセスする ACS のバージョンに対応したリリース ノートを参照してください。リリース ノートの最新版は、Cisco.com に掲載されています。

UCP Web ページの URL は次のとおりです。

`http://webserver/secure/login.htm`

ここで、`webserver` は UCP を実行している Web サーバのホスト名または IP アドレスであり、`secure` は P.1-3 の「Web サーバの準備」で作成した `secure` 仮想ディレクトリ エイリアスです。



ヒント

UCP ページへの URL を短くするには、Web サーバ上のデフォルト ドキュメントに `login.htm` を付加します。この場合、URL は `http://webserver/secure` となります。

UCP のアップグレード

UCP ソフトウェアをアップグレードするには、次の手順を実行します。

- ステップ 1** P.1-9 の「UCP のアンインストール」の手順を実行して、旧バージョンの UCP をアンインストールします。
- ステップ 2** P.1-4 の「UCP 向けの Cisco Secure ACS の準備」の手順を実行します。
- ステップ 3** アップグレードする新しいバージョンの UCP を使用して、P.1-3 の「UCP のインストール」の手順を実行します。

UCP のアンインストール

User-Changeable Password ソフトウェアをアンインストールするには、次の手順を実行します。

- ステップ 1** UCP を実行しているコンピュータ上で、**Windows Control Panel > Add or Remove Programs** を選択して ACS User-Changeable Password をアンインストールします。
- ステップ 2** IIS で、UCP の HTML ファイル用および CGI ファイル用に作成した仮想ディレクトリを削除します。これらのディレクトリのデフォルト名は、**secure** と **securecgi-bin** です。ただし、UCP のインストール時にディレクトリ名をカスタマイズしている可能性もあります。
- ステップ 3** 仮想ディレクトリがマップされていたディレクトリが削除されたことを確認します。この削除は、**ステップ 1** で行われます。ディレクトリが削除されていない場合は、ここで削除します。
- ステップ 4** Web サーバが IIS 6.0 を実行している場合は、IIS で未知の CGI 拡張機能を継続して許可するかどうかを検討します。この設定を変更するには、IIS Manager ウィンドウの Web Service Extension ページを使用して、**Allow Unknown CGI Extensions** のステータスを変更します。
- ステップ 5** ACS の HTML インターフェイスで、UCP を実行していたサーバに対応する AAA サーバ設定を削除します。AAA サーバ設定の削除方法については、使用しているバージョンの ACS のユーザガイドを参照してください。

パスワードの変更



(注) パスワードを変更するための適切なアクセス権が付与されていることを、システム管理者に確認してください。

Web サーバを使用してパスワードを変更するには、次の手順を実行します。

ステップ 1 Web ブラウザを起動し、管理者から通知された URL を使用して UCP ページを開きます。

ステップ 2 ユーザ名とパスワードを入力し、次に **Submit** をクリックします。

Change Password ページが開きます。前のページで入力したユーザ名が Username ボックスに表示されます。

ステップ 3 次のように入力します。

- **Current Password** : 現在のパスワードを入力します。
- **New Password** : 新しいパスワードを入力します。



(注) パスワードは、最小文字数など、特殊な要件を満たさなければならない場合があります。詳細については、システム管理者に問い合せてください。

- **Confirm New Password** : 新しいパスワードを再入力します。

ステップ 4 **Submit** をクリックします。

パスワードが変更されます。

ステップ 5 **Logout** をクリックして終了します。



け

警告

意味 vi

ち

注意

意味 vi

ひ

表記法 vi

ま

マニュアル

表記法 vi